Service Organization Control SOC 2, Type 2 Report

Report on Controls at a Service Organization Relevant to the following Trust Service Principles:

Security, Availability, Processing Integrity and Confidentiality

January 1, 2014 to December 31, 2014

Table of Contents

eDelta CPA Services, P.C.
380 Lexington Avenue, Suite 608
New York, New York 10017

Phone: 646-205-9960
Fax: 631-389-2395

Section I: Independent Service Auditors' Opinion Letter

To: The Management of Highstreet
Islandia, New York

Scope:

We have examined Highstreet description of general computer controls related to their Co-location Facility Network Operations Center and supporting IT Services ("Services") located in Islandia, New York for the period January 1, 2014 to December 31, 2014 ("Description") and the suitability of the design and operating effectiveness of controls stated in the Description. The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls contemplated in the design of Highstreet's controls are suitably designed and operating effectively. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Highstreet Responsibilities:

In Section II of this Report, Highstreet has provided an assertion about the fairness of the presentation of the Description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the Description ("Assertion"). Highstreet is responsible for preparing the Description and for the Assertion, including the completeness, accuracy, and method of presentation of the Description and the Assertion and stating the control objectives in the Description. Highstreet is also responsible for the Services covered in the Description, specifying the control objectives, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the Assertion and designing, implementing and documenting controls to achieve the related control objectives stated in the Description.

Service Auditor's Responsibilities:

Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the Description, based on our examination. We conducted our examination in accordance with the Statements on Standards for Attestation Engagements No. 101 ("AT 101") and Service Organization Control ("SOC" 2) established by the American Institute of Certified Public Accountants ("AICPA").

Those standards require that we comply with ethical standards and plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the Description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the Description throughout the period January 1, 2014 to December 31, 2014.

eDelta CPA Services, P.C.
380 Lexington Avenue, Suite 608
New York, New York 10017

Phone: 646-205-9960
Fax: 631-389-2395

An examination of a Description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls to achieve the related control objectives stated in the Description involves performing procedures to obtain evidence about the fairness of the presentation of the Description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the Description.

Our procedures included assessing the risks that the Description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the Description. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the Description were achieved. An examination engagement of this type also includes evaluating the overall presentation of the Description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described in the Assertion. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations:

The Description is prepared to meet the common needs of a broad range of user entities and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in its own particular environment. Because of their nature, controls at the service organization may not prevent, or detect and correct, all errors or omissions in the Services provided by Highstreet. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives is subject to the risk that controls at the service organization may become inadequate or fail.

Opinion:

In our opinion, in all material respects, based on the criteria described in Highstreet's Assertion:

A. The Description, in Section II of this Report, fairly presents the Services for user entities that was designed and implemented throughout the period January 1, 2014 to December 31, 2014.

B. The controls related to the control objectives stated in the Description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period January 1, 2014 to December 31, 2014 and if user entities applied the complementary user entity controls contemplated in the design of Highstreet's controls throughout the period January 1, 2014 to December 31, 2014.

C. The controls tested, in Section III of this Report, which together with the complementary user entity controls referred to in Section II of this Report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the Description were achieved and operated effectively throughout the period January 1, 2014 to December 31, 2014.

eDelta CPA Services, P.C.
380 Lexington Avenue, Suite 608
New York, New York 10017

Phone: 646-205-9960
Fax: 631-389-2395

Description of Tests of Controls:

The specific controls tested and the nature, timing, and results of those tests are listed in Section III of this Report.

Restricted Use:

This Report, including the description of tests of controls and results thereof in Section III, is intended solely for the information and use of Highstreet Management, user entities of Highstreet during some or all of the period January 1, 2014 to December 31, 2014, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This Report is not intended to be and should not be used by anyone other than these specified parties.

June 30, 2015

eDelta CPA Services, P.C.

eDelta CPA Services, P.C.

SECTION II – Description of Internal Controls Provided by Highstreet

MANAGEMENT'S ASSERTION, DECEMBER 31, 2014

We have prepared the description of Highstreet's general computer controls related to our Co-location Facility Network Operations Center and supporting Information Technology (IT) Services ("Services") located in Islandia, New York for the period January 1, 2014 to December 31, 2014 (the "Description") and the suitability of the design and operating effectiveness of controls stated in the Description, and for the notified auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, in connection with this report. In connection with this report, we confirm, to the best of our knowledge and belief, that:

A. The Description in this report fairly presents Highstreet Services made available to user entities of Highstreet during some or all of the period January 1, 2014 to December 31, 2014. The criteria we used in making this assertion were that the Description:
   I. Presents how Services made available to user entities were designed and implemented to process relevant transactions, including:
      1. How Services are initiated with user entities;
      2. Security controls (Information and Physical Security);
      3. Physical Security controls (access to the Highstreet Co-location Facility);
      4. Availability controls (environmental controls and redundant power systems provided to user entities);
      5. Processing controls (monitoring);
      6. Confidentiality controls;
      7. Specified control objectives and controls designed to achieve those objectives and,
      8. Other aspects of our control environment, including governance, risk assessment, monitoring and communication.
   II. Does not omit or distort material information relevant to the scope of Highstreet's Services, while acknowledging that the Description is prepared to meet the common needs of a broad range of user entities of the Services and the independent auditors of those user entities, and may not, therefore, include every aspect of Highstreet Services that each individual user entity of the Services and its auditor may consider important in its own particular environment.

B. The Description includes relevant details of changes to the service organization's Services during the period covered by the Description when the Description covers a review of time.

C. The controls related to the control objectives stated in the Description were suitably designed and operated effectively throughout the review period January 1, 2014 to December 31, 2014, to achieve those control objectives.

The criteria we used in making this Assertion were that:

I. The risks that threaten the achievement of the control objectives in the Description have been identified by the service organization.
II. The controls identified in the Description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the Description from being achieved; and,
III. The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

OVERVIEW OF OPERATIONS

Highstreet is a professional services and maintenance organization providing full Information Technology (IT) enterprise service solutions and support to middle market companies and small businesses. Highstreet IT services include the following:

- Server Hosting (Collocation);
- Network Operations;
- Security Operations;
- Hardware and Software Maintenance;
- IP Telephony;
- Application Development; and,
- Professional Services.

Highstreet is headquartered in Islandia, New York, with offices in Manhattan, Hillsdale, New Jersey and Delaware. It partners with industry leaders, including: Cisco, IBM, HP, EMC and Oracle/Sun Microsystems in order to deliver products and services to its' Clients. Highstreet services are provided by its' internal Information Technology and Security Department (ITS), and also through its' Network Operations Center (NOC).

The ITS Department provides the following services:

- Information Technology Policies, Procedures and Standards;
- Network and Server Management, and Administration (including Performance and Capacity);
- Infrastructure Upgrades and Software Updates (including Patch Management); and,
- Business Continuity and Disaster Recovery.

The NOC is comprised of the following services:

- Network and Server Monitoring;
- Client Portal Management and Administration; and,
- Service and Help Desk Support.

IT infrastructure components utilized to support Client organizations are listed below:

Infrastructure System	Description
Cisco Pix	Active/Passive Firewall(s) for (Client) subnet
Cisco ASA	Active/Passive Firewall(s) for (NOC) subnet
ISA Server	Software Firewall Management
Barracuda	Anti-Spam Device
Citrix	Remove Access Server

Highstreet Applications/Tools

Highstreet applications/tools in use are listed below:

Applications/Tools	Description
Remote Access	
Cisco VPN Client	Cisco VPN Client: enables Engineers to access the Highstreet network from a remote location.
Network and Server Management	
Secure CRT	Secure CRT: is a terminal emulation application with the strong encryption and a broad range of authentication options. It also provides data integrity for the Secure Shell.
Netsupport	Netsupport: is PC remote control software with multi-platform capability.
VNC Viewer	VNC Viewer: is PC remote control that allows users to remotely control desktop applications across any network.
Devolutions Remote Desktop Manager	Devolutions Remote Desktop Manager: is an Open Source Remote Desktop Protocol (RDP) management tool.
Network and Server Monitoring	
Nimsoft	Nimsoft: is monitoring software for the NOC Client network devices.
Wireshark	Wireshark: is an Open Source packet sniffing tool.
Network and Client Communications	
Cisco Desktop Agent	Cisco Desktop Agent: is an IP Telephony application with call control capabilities (i.e. call answer, hold, conference, and transfer, ACD state control, ready/not ready, wrap up, etc..).
Cisco Desktop Supervisor	Cisco Desktop Supervisor: is an application that enables users to monitor Cisco Desktop Agents.
Pidgin	Pidgin: is a multi-protocol instant messaging Client for Windows. Pidgin messenger is compatible with AIM and ICQ (Oscar protocol), MSN Messenger, Yahoo!, IRC and networks.
Virus Protection	
Trend Micro	Trend Micro: is the Enterprise Anti Virus software used by Highstreet.
Field Engineers Laptops	
Solar Winds TFTP	Solar Winds TFTP: enables Engineers to upload and download executable images and configurations to network devices.
Crystal Reports	Crystal Reports: provides server and network activity reports from a wide range of network and server data sources.
Microsoft Navision	Microsoft Navision: is used to manage Highstreet Dispatch/Service group's dispatch calls, Client calls, and provide field Engineer time reporting.
Secure CRT	Secure CRT: provides terminal emulation with the strong encryption, a broad range of authentication options, and data integrity of the Secure Shell.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT

Communication and Enforcement of Integrity and Ethical Values

Highstreet strives to achieve a culture and climate of high integrity by clearly communicating expectations, monitoring performance against expectations, and setting the right example at the top. All employees are required to review and acknowledge Highstreet's policy as a condition to employment.

Integrity and Ethical Values

Highstreet has a Code of Ethics Policy to educate employees on business ethics, conflicts of interest, compliance with laws and the handling of confidential and proprietary information. Human Resources and the Executive Committee, comprised of the President and COO; are responsible for developing the Code of Ethics Policy at Highstreet. All Highstreet policies, guidelines, diagrams, references and manuals are available electronically on the Corporate Compliance SharePoint Site. Critical policies include, but are not limited to the:

- Security Policy;
- Change Management Policy;
- Business Continuity and Disaster Recovery Plan;
- Building Access Policy; and,
- Employee Handbook.

Assignment of Authority and Responsibility:

The organizational structure at Highstreet is designed to facilitate information flow and increase Highstreet's ability to respond to both Client needs and other important issues. The Highstreet organizational structure supports:

- Departments defined by operational tasks, and managers and staff responsible for implementation; and,
- Departmental/cross-departmental teams established to handle a particular activity.

Highstreet Senior Management meets on a regular basis to discuss and review organizational initiatives that are either planned or in process, as well as to discuss outstanding issues and/or concerns. In addition to regularly scheduled meetings, an internal phone call (chain method) is used at Highstreet to notify appropriate Management should a critical issue occur.

Policies and Practices:

Highstreet utilizes a subset of the ISO/IEC 27002:2005 framework (formerly known as ISO 17799:2005) for IT internal controls. The ISO/IEC 27002:2005 framework establishes guidelines and general principles for managing and improving information security processes, and is comprised of the following:

- Security Policy;
- Organization of Information Security;
- Asset Management;

Policies and Practices (Continued):

- Human Resources Security;
- Physical and Environmental Security;
- Access Control;
- Communications and Operations Management;
- Information Systems Acquisition, Development and Maintenance; and,
- Information Security Incident Management.

Expectations regarding employee integrity and conduct are communicated to employees through an Employee Handbook, which is posted on Highstreet's Corporate Compliance SharePoint Site. The contents of the Employee Handbook are reinforced through ongoing training provided by Supervisors and Management throughout Highstreet.

The Highstreet Code of Ethics Policy is distributed to all new employees, and a formal new employee indoctrination program which describes internal controls is provided to new employees by Human Resources. Executive and Departmental Management, including Information Technology, reviews the Employee Handbook and related policies and procedures on an annual basis, and requires that employees sign-off and acknowledge that they have read and understand these policies.

Deviations from established policies and/or procedures are escalated to Highstreet Senior Management. Additionally, Highstreet Supervisors are encouraged to provide staff feedback immediately for non-conformance with Highstreet policies. Members of Highstreet Senior Management are engaged when recurring performance concerns are identified. Annual performance reviews are also completed for selected Departments within Highstreet, including the NOC, Back Office Processing and Field Services.

Highstreet maintains a budget for education and ongoing training programs, which is established based on both organizational need and the employee's career path. The purpose of training programs is to keep key personnel up-to-date with the latest technology and tools used within the NOC and the equipment deployed by their Clients. Ongoing employee education and training is also a factor in the annual performance review process.

Information and Communication:

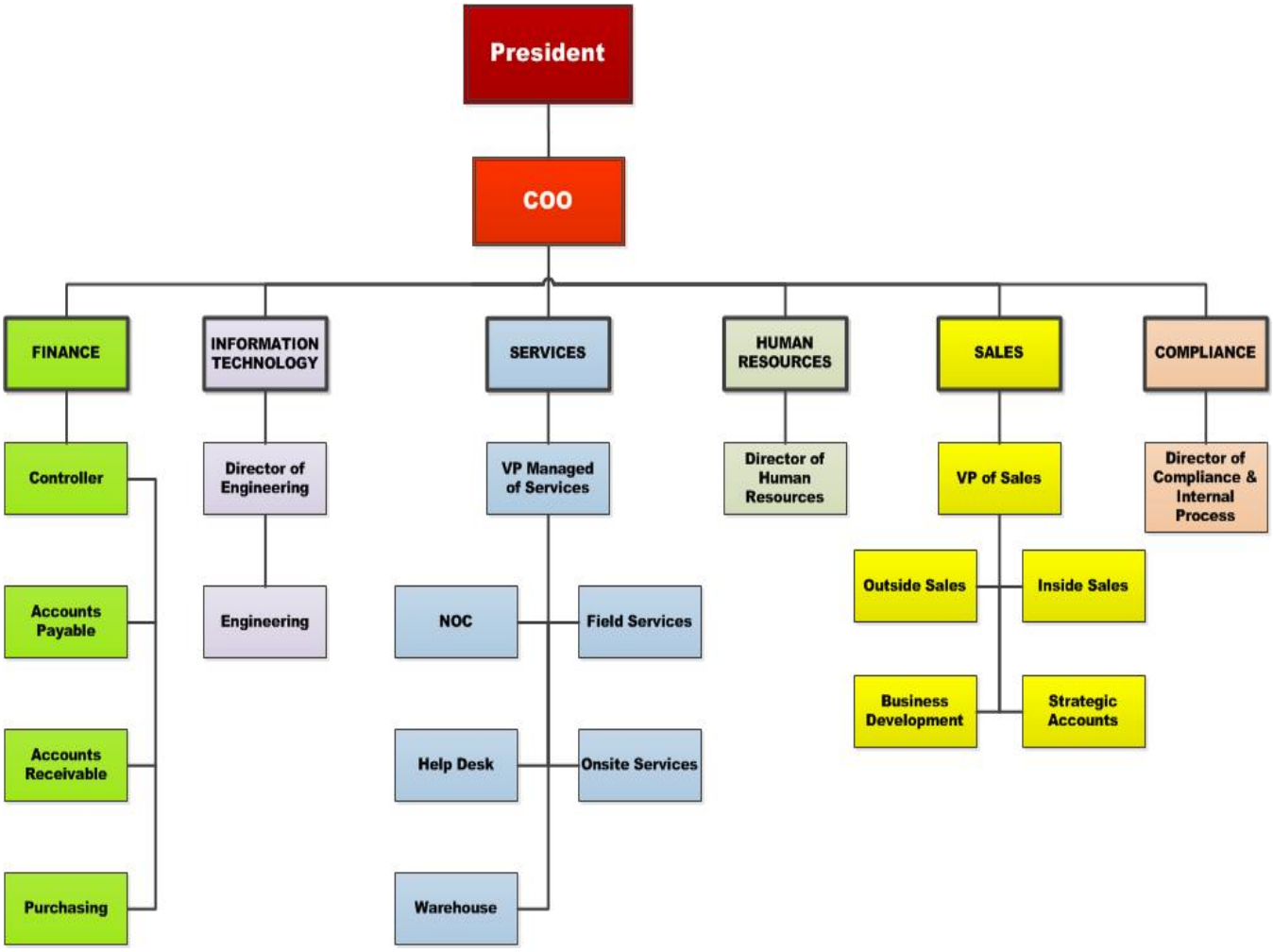
Highstreet Management reviews its policies, procedures and standards periodically (and at a minimum, annually) to reflect changing business conditions. A formal annual compliance assessment is performed by Highstreet whereby key business processes are reviewed and exceptions are documented. This assessment includes: identifying the root cause, the remedial action required and tracking remediation actions to completion.

Monitoring:

The Executive Committee is comprised of the President and COO, and regularly provides information about the functioning of internal controls at Highstreet. Ongoing monitoring activities are also built into the normal activities performed at Highstreet.

Organizational Structure

Figure 1 – Organization Chart:



IT Department Overview

IT Governance and Risk Management:

The IT planning approach includes mechanisms to solicit input from relevant stakeholders affected by IT strategic plans, and to communicate these plans to business process owners and other relevant stakeholders. IT Management communicates its activities, challenges and risks on a regular basis to the business. Additionally, relevant IT systems and data are inventoried and their owners identified. Highstreet has identified qualified IT Managers who demonstrate the required knowledge and experience to fulfill their responsibilities. Highstreet IT Managers must be conversant in Business Continuity, Disaster Recovery and Change Management concepts, and be able to periodically assess information risk. Highstreet routinely considers the probability and likelihood of stakeholder threats at a high level.

IT Monitoring:

Documentation is created and maintained for significant IT processes, controls and activities. A consistent quality assurance plan exists for significant IT functions, including: Change Management, Systems Acceptance and Patch Management activities that address general and project-specific monitoring concerns. Highstreet Management also utilizes the Capacity Management and Change Management functions, as well as weekly Manager Meetings, to monitor the delivery of Information Technology Services (ITS).

Organization of Information Security

With regards to Information Security, the Highstreet ITS Department is responsible for:

- Reviewing, assessing and enforcing the Highstreet Security Policy;
- Physical facility and logical network access management, including:
  - New user setup;
  - Modifications to existing user access; and,
  - Removal of terminated user access.
- Management and support of firewalls, servers and other networked devices. Highstreet also offers and performs Cisco support including, but not limited to:
  - File and directory services maintenance and usage/security monitoring; and,
  - Phone setup, configuration and the use and quality of service management.
- Establishing and monitoring internet and network connectivity both internally and externally;
- Providing capacity management (via Nimsoft) for Exchange servers, SQL database servers, NOC PC and dedicated security appliances, Domain Controllers, WSUS patch management servers, Citrix and RADIUS servers;
- The protection of core servers and services against the threat of virus and spyware attacks;
- Performance of the infrastructure change management processes, including patch management;
- Providing Helpdesk Levels 1, 2, and 3 support for internal hardware, including servers, desktops and laptops, printers, and other peripherals;
- Providing basic training and support for email servers, and Citrix, and VPN connections;
- Assessing and reporting incident trends with recommendations for improvement; and,
- Providing primary support and coordination for Business Continuity and Disaster Recovery planning.

Highstreet has published security goals within its Security Policy and Security Charter. Roles and responsibilities for information security are defined within the formal employee job descriptions.

Information Security Responsibility

Information Security is governed and monitored by a designated member of the Highstreet Management Team. A Security Committee Management Team meets on a regular basis to address corporate security concerns and internal policies.

Security Policy

Highstreet has an approved Security Policy available internally to all employees which considers the organization's business operations, including regulatory, statutory and organizational requirements. The Security Policy is owned by the Office of Information Technology and Security (OITS) who is responsible for the review and/or update of the Security Policy on an annual basis. The Security Policy is signed and approved by the Security Committee. All changes to the Security Policy are documented on the Policy's revision page. The Security Policy is distributed to employees through an email message and is reinforced during Security Awareness training sessions that are conducted on an annual basis.

The importance of adherence to all provisions of the Security Policy is detailed within the Security Charter. New employees receive a copy of the Security Policy upon hire. The Security Policy covers the following key areas with respect to Client data:

- Access - Only System Administration personnel are allowed to access Client databases. Employees are not allowed to have unencrypted access to an end Client's user ID or password, and may not attempt to view copy, print, store, or share with a third party any sensitive Client information (including biographic information, social security number, financial transaction information (balances, net worth, debt, etc.)) without authorization given by the Office of Information Technology and Security and the owner of the data. All such data must be encrypted in storage and in transit.
- Log files are required to be maintained for a period of three months, and must be secured and periodically reviewed to comply with the Highstreet Security Policy.
- SSL (Secure Sockets Layer) or an equally secure encryption method is required for end Client access to Highstreet or a co-branded service. SSL is required when fetching end Client data from the end Client site whenever the third party site allows SSL connections, and uses 128 bit encryption (as the standard) with 40 bit encryption (only when gathering data from an end Client site that is limited to 40 bit encryption).
- Paper documents are required to be securely stored in locked containers prior to their destruction. The locked containers are emptied as required by an independent vendor and taken to a destruction site. Highstreet employees are required to immediately shred any documents with confidential data.
- The Highstreet Security Policy requires the secure disposal of unwanted media. Used computer media is to be physically destroyed before it is thrown away. Hard drives are securely overwritten using a DOD compliant disk wiping utility. Used computers are removed by an independent vendor that certifies that all data has been erased.
- Highstreet has a written Policy that requires users to clear their desk and work areas of sensitive or critical business operations information when the user no longer occupies the area.
- A VPN and Dial-in Access Policy requires that inbound dial-up lines connected to Highstreet internal networks and/or computer systems pass through an additional access control point (such as a firewall) that has been approved by the Highstreet Information Security Department (before users reach the log-in banner).

- An Internet/Email Content Policy requires that Highstreet electronic media (including the Internet and email) not be used to:
  - Send out Highstreet classified, proprietary or trade secret data without proper authorization;
  - Send out end Client or partner information without proper authorization; and,
  - Engage in an activity that is in violation of local, state or federal law.
- Communicate, store or view inappropriate or unacceptable material. Examples of inappropriate or unacceptable material include, but are not limited to:
  - Offensive or harassing statements or language;
  - Sexually explicit messages or images;
  - Disseminating or printing copyrighted materials, violating copyright laws; and,
  - Downloading material from an untrusted source that could potentially harm Highstreet computer resources or data.
- A software Virus Protection Policy requires that virus screening software be installed and configured to run periodically on all Highstreet mail servers, firewalls, intranet servers, laptops, workstations and desktop machines. Virus detection software must be kept up-to-date using automated means where new virus signatures/virus definitions are added as they are discovered by the virus detection software vendor.
- A Network Configuration Policy is established so that router and firewall business rules and configurations are accurately documented and readily available for review.
- Highstreet has published and distributed a graduated disciplinary process for security breaches to all employees in the Employee Handbook.

Asset Management

Highstreet maintains an asset tracking application called Total Network Inventory (TNI), which is updated every six months. The accuracy of the inventory is verified using network scans to determine if all network assets are identified and cataloged. All assets are assigned to a Highstreet Technology and Business Owner.

Roles and responsibilities for Technology and Business Owners are documented in the Highstreet Security Policy and in the individual asset owner's job descriptions. Technology owners are responsible for ensuring that the assets comply with the Highstreet Security Policy. Business owners are responsible for reviewing access restrictions and classifications, taking into account applicable access control policies.

Human Resources

Background checks are performed on all Highstreet employees, contractors and third parties in accordance with their roles and responsibilities, job function and level of access to sensitive or classified information. Every employee, as well as contractors and third-parties, are required to sign a Confidentiality/Non-Disclosure Agreement as a condition of employment and/or statement of work. Confidentiality/Non-Disclosure Agreements are stored in the employee's personnel file or within the Legal Department.

Highstreet has a formal Security Awareness education and training program for employees, contractors and relevant third party resources. The Security Awareness program is required to be taken prior to an employee being assigned access rights to sensitive information and information systems. The Highstreet Security Awareness education and training program includes key elements such as: security requirements, legal responsibilities, incident reporting, and business controls.

Employees are required to take the Security Awareness program on an annual basis. Attendance records for the Security Awareness program are maintained indefinitely in an employee's personnel file. Contractors and relevant third parties are also required to take Security Awareness education and training based on their exposure to sensitive and classified information at Highstreet.

Physical Security

All Highstreet building facility perimeter and fire exit doors are alarmed, monitored and tested periodically to ensure operational functionality. The delivery and loading area is also physically separated from the remainder of the Highstreet administrative office.

Access to Highstreet administrative offices and the Data Center are controlled through an electronic card access system. Sensitive areas, including the Data Center, are further protected through the use of biometric devices. These systems record the date, time, entry and the departure of all employees. Employees can only access areas where they have a legitimate need based on their job responsibilities. All visitors and vendors must sign in at a manned reception desk and must be escorted at all times while in the building. Highstreet maintains a policy requiring all employees, contractors and third party visitors and vendors to wear a visible identification badge.

Security cameras are used to monitor security and compliance at all perimeter doors and at the Data Center, as well as to record activities on a 24 x 7 basis to a digital video recorder (that is backed up to read-only media daily and stored in a secure location).

Environmental Controls

The Data Center is cooled by a separate refrigeration system, which is connected to backup natural gas generators. The Data Center and administrative offices are protected by a Novec fluid system which extinguishes by removing heat from the fire. The Data Center also has a fire alarm that is monitored by central station on a 24 x 7 basis.

Computer systems are connected to an Uninterrupted Power Supply (UPS) to support the orderly shutdown of systems and/or the continuous running of systems as appropriate. Highstreet has a backup natural gas generator in place for critical systems requiring extended continuous operation to support business requirements. The backup generator is tested on a quarterly basis and is connected to a direct feed natural gas line for continuous activity.

Emergency lighting exists in the Data Center, as well as the core information processing facilities, in the event of a major power failure. Power and telecommunications lines into Data Center and core information processing facilities are buried underground to reduce the risk of damage to them.

Paper documents and/or other flammable materials are kept outside of the Data Center and/or core information processing facilities and aisles and/or major walkthroughs are free from obstruction and other electrical hazards.

Communications and Operations Management

Highstreet maintains Operating Procedures for information systems which are available to users on the Highstreet network. These Operating Procedures cover the processing and handling of information, including backup and restore, system startup and the shutdown and handling of other electronic media.

Nimsoft is used to monitor the Data Center, and is configured to provide alerts via email, SNMP, Text Messaging, HTTP and Web Services. Customized alert actions are configured based on alert type, severity and time the alert occurred. Highstreet has configured capacity alerts on important systems to warn administrators if processor utilization or hard drive capacity exceeds established thresholds.

All clocks on information systems are synchronized via the Network Time Protocol (NTP) to ensure the integrity and accuracy of systems.

Access Controls

Highstreet maintains a distributed Access Control Policy requiring specific actions before access can be granted to information systems. The access rules and rights for each user and group are documented and communicated to all new employees. The Access Control Policy covers both logical and physical security elements. Access rights are granted on a need-to-know basis.

Highstreet utilizes a formal process for user registration and de-registration for the granting and revoking of access rights to all information systems and services, and all access requires managerial pre-approval. Highstreet Management conducts a review of access controls for all types of users every six months. User Access rights are also removed or disabled after a period of inactivity. A formal termination process exists to ensure the proper return of all previously issued corporate assets under the control of the employee (or a third party) and the termination of all accounts.

Highstreet maintains a complex password policy for it systems and servers. The Highstreet Account and Password Policy prohibits' passwords from being communicated through electronic mail, and provides guidance to users in selecting a password. Also, passwords are to be stored in an encrypted format on the system and are to be separate from system data. Users are required to terminate their session when finished, even if they are still in their respective work area. Workstations are also configured to logoff after a period of inactivity.

Security Standards

Security standards with regards to mobile computing and communications are a standard part of Highstreet's Security Awareness training program. Highstreet has established an Acceptable Use Policy with rules for the use of mobile devices, email, internet services and instant messaging. Violations of the Acceptable Use Policy include penalties up to and including termination, based on the outcome of incident investigations.

Remote access is controlled through a Virtual Private Network (VPN). Highstreet uses encrypted VPN technology or similar controls for securing remote network connectivity. All wireless devices utilize the WPA encryption protocol. Additionally, the SSID is not broadcasted, and all devices have had their default passwords changed.

Highstreet protects system diagnostic and configuration ports through the use of secure login accounts and passwords. Firewalls and security devices such as: IDS, virus filtering, and encrypted/complex authorization mechanisms exist to prevent unauthorized users from connecting to the VPN, Citrix service and/or network devices. Firewalls are configured to deny inbound traffic by default, with only designated ports and protocols enabled to support access based on justified business needs.

Highstreet utilizes a third party entity to scan, detect, assess and remediate any security vulnerabilities on the network. This software scans the entire network to identify possible security threats and provide recommendations to remediate the identified vulnerabilities.

Information Security Monitoring and Incident Management

Highstreet has established a formal incident reporting process in the Security Policy, which documents escalation plans and procedures to quickly report information security incidents. Employees, contractors and third parties are required to note and report any observed or suspected security weaknesses in information systems or services to the Information Technology and Security Department. Security incidents are recorded and tracked centrally by the Information Technology and Security Department.

The procedure for the reporting of information security incidents is also a standard part of Information Security Awareness training for all users. There is also a documented formal disciplinary process defined in the Employee Handbook for users who commit security breaches.

Highstreet operations staff actively monitor the intrusion detection system for possible intrusions on a 24/7 basis. Upon detection of any suspicious activity, an investigation and analysis of the possible causes is conducted. Should Highstreet determine that there is a possible hacker attack; the incident handling process will be activated. Failed authentication alerts are also monitored. If the number of invalid user logon attempts are exceeded, the system administrators will be alerted and follow-up as to the potential cause.

Information Backup and Restore Processes

Management has defined guidelines for laptops and other mobile devices in its Security Policy and has defined information backup policies for all critical environments. Full backups are taken on a nightly basis, and backup media is tested on a monthly basis to ensure its availability and correctness. Backup Tapes are picked up Monday through Friday and are stored securely offsite. Backup tapes are also stored in secure locked containers during their transit to the offsite facility.

Compliance to the Security Policy

The Highstreet Information Technology and Security Department is responsible for keeping Management up-to-date and Highstreet in alignment with all relevant statutory, regulatory and contractual requirements. IT compliance with the Security Policy is monitored by a designated individual at Highstreet. The following key measures are in place:

- Management requires the legal use of software and information products. Highstreet routinely performs reviews by utilizing automated auditing software to verify that only authorized software products are installed.
- Highstreet is required to protect important records from loss, destruction, and unauthorized modification in accordance with applicable statutory regulatory, contractual and business requirements. Records are destroyed after the retention period has expired.
- Highstreet information systems display a warning banner message that “systems are owned by the organization and unauthorized use against policy”.
- Highstreet conducts independent internal and external vulnerability scanning to ensure compliance with security standards.
- Third party contracts and agreements include language that requires third parties to comply with the Highstreet Security Policy. A copy of the Security Policy is provided and communicated to all third party vendors and partners.

Risks that May Threaten the Achievement of Control Objectives

Specific application and information technology related controls were selected by Highstreet Management for review in Section III of this Report. Highstreet Management feels that the selected Control Objectives address concerns in the market place for independent assurance on the reliability of Highstreet Services. However, there are certain risks that Highstreet has identified that pose a threat to the achievement of the Control Objectives stated in Section III of this Report.

These include, but are not limited to, the following:

- Catastrophic regional and national damage to facilities by acts of nature, such as flood, wind, fire and earthquake at Highstreet’s primary Colocation Facility in Islandia, New York;
- Adverse changes in economic conditions;
- Regional or national failure of the power grid;
- Acts of war, sabotage or terrorism; and,
- Local and regional pandemic outbreaks.

DESCRIPTION OF CONTROLS

Highstreet Management has defined the following Control Objectives and Control Activities:

Control Objective #1:

- Controls over the administration, management and support of information security provide reasonable assurance that they are in accordance with business requirements and relevant laws and regulations.

Control Activities:

Code of Ethics Policy:

A Code of Ethics Policy in the Employee Handbook exists at Highstreet to educate employees on Highstreet's position regarding business ethics, conflicts of interest, compliance with laws, and the handling of confidential and proprietary information. Human Resources is responsible for implementing the Code of Ethics at Highstreet. **(1.1)**

Security Policy:

The Security Policy document is approved by Highstreet Management, and is published and communicated to all employees and relevant external parties. **(1.2)**

Governance:

Senior Management meets on a regular basis to discuss and review organizational initiatives that are either planned or in process, as well as to discuss outstanding issues and/or concerns. **(1.3)**

Service Level Agreements:

Service Level Agreements (SLA's) are in effect with clients and third parties indicating the levels of support to contractors and relevant third parties. **(1.4)**

Liability Insurance:

Liability Insurance is in effect with declarations supporting reasonable coverage for Highstreet. **(1.5)**

Control Objective #2:

- Controls provide reasonable assurance that a management framework is established to initiate and control the implementation of information security within Highstreet.

Control Activities:

Incident Response:

An information Security Incident Response Policy document is approved by Management, published and communicated to all employees and relevant external parties. **(2.1)**

Security Responsibilities:

The Security Policy clearly defines specific the requirements and responsibilities of information for Highstreet personnel. Formal job descriptions are in place, which define all security roles and responsibilities. **(2.2)**

Implementing Security:

Highstreet's approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes and procedures for information security) are reviewed independently at planned intervals by Management, or when significant changes to the security implementation occur. Alert Logic performs internal scanning. **(2.3)**

Control Objective #3:

- Controls over organizational assets provide reasonable assurance that they are properly classified to protect against their misuse.

Control Activities:

Acceptable Use Policy:

Rules for the acceptable use of information and assets associated with information processing facilities are identified, documented in the Acceptable Use Policy, and are implemented by Highstreet Management. **(3.1)**

Classification of Information:

Information Systems Management and Administration Information is classified in terms of its value, legal requirements, sensitivity and criticality to Highstreet. **(3.2)**

Control Objective #4:

- Controls over disciplinary actions and the termination of employees, contractors, and 3rd party users provide reasonable assurance to reduce the risk of theft, fraud or misuse of facilities.

Control Activities:

Performance and Employee Termination:

Members of Senior Management are engaged when recurring performance concerns are identified. Annual performance reviews are completed for selected departments within Highstreet, such as, NOC, Back Office Processing, and Field Services. Responsibilities for performing employment termination or change of employment are clearly defined, assigned and documented by Management. **(4.1)**

There is a formal disciplinary process for employees who have committed a security breach. This disciplinary action is documented in the Security Policy. **(4.2)**

Control Objective #5:

- Controls provide reasonable assurance that physical access to organizational premises, data center facilities and other sensitive operational areas are restricted to authorized users.

Control Activities:

Building Security:

Security perimeters, including barriers such as walls and manned reception desks are used to protect areas that contain Highstreet information and the information processing facilities. **(5.1)**

Card Key and Biometric Access:

Physical access to the Highstreet building facility is restricted through card key access. Access to the NOC is restricted through both card key and biometric access. **(5.2)**

Visitor and Vendor Access:

Visitors and vendors entering the Highstreet building facility must go to the reception desk where they enter their name, company information, the reason for their visit, and the time of their visit and date in a sign-in log. **(5.3)**

The receptionist contacts the appropriate Highstreet representative who escorts the vendor or visitor to the appropriate location. **(5.4)**

Visitors and vendors are required to wear an ID badge which identifies them to Highstreet personnel. **(5.5)**

Monitoring Physical Access:

Physical access to the Highstreet building facility and the NOC are monitored and reviewed on a periodic basis by Highstreet Management for any unusual activity. **(5.6)**

Video surveillance cameras are in place to monitor any unusual activity for the Highstreet building facility and NOC. Security surveillance equipment is inspected and maintained to ensure proper operation. **(5.7)**

Security Alarms:

The Highstreet building facility and the NOC are alarmed for physical security breaches. Should an intruder break-in take place, a message is sent to the proper authorities (i.e., the police and fire departments) for further action. **(5.8)**

Physical Access Points:

Access points, such as delivery and loading areas and other points (where unauthorized persons may enter the premises) are segregated from the Highstreet information processing facilities to help avoid unauthorized access. **(5.9)**

Authorization for Removal of Assets:

Equipment, information and software are not taken off-site without prior authorization from Highstreet Management. **(5.10)**

Control Objective #6:

- Controls provide reasonable assurance that environmental controls are established within the data center and processing facilities to protect physical assets.

Control Activities:

Temperature Control and Power Backup:

The Highstreet Data Center is cooled by a separate refrigeration system that is connected to separate backup natural gas generators should an electrical outage occur. **(6.1)**

Fire Prevention and Monitoring:

The Data Center and administrative offices are protected by a Novec fluid system which extinguishes by removing heat from the fire. The Data Center also has a fire alarm that is monitored by a central station on a 24 by 7 basis. **(6.2)**

Water Detection and Flood Protection:

Water detection sensors are provided in the Data Center and alerts are sent to Highstreet Management should water be detected. **(6.3)**

Heat Detection:

Heat detection sensors are provided in the Data Center and alerts are sent to Highstreet Management for any unusual at temperature conditions. **(6.4)**

UPS and Power Redundancy:

Equipment is protected from power failures and other disruptions caused by failures in supporting utilities, through an Uninterrupted Power Supply (UPS), which is phased to a backup gas generator to help ensure continued operations. **(6.5)**

Emergency Lighting:

Emergency lighting exists in the Data Center as well as core information processing facilities in the event of a major power failure. **(6.6)**

Location of Power and Telecommunication Lines:

Power and telecommunications lines into Highstreet Data Center and core information processing facilities are buried underground to reduce the risk of significant damage to them. **(6.7)**

Fire Safety Measures:

Paper documents and other flammable materials are kept outside of the Highstreet Data Center and core information processing facilities. Aisles and major walkways are also free from obstruction and other electrical hazards. **(6.8)**

Control Objective #7:

- Controls over the operation and monitoring of information systems provide reasonable assurance that data is processed completely and securely.

Control Activities:

Authorization and Approval of Changes:

Changes to information processing facilities and systems are documented, and require formal authorization and approval from Highstreet Management on the change control tracking form before they are implemented. **(7.1)**

Problem Monitoring and Corrective Actions:

Procedures and automated tools for monitoring the use of information processing facilities are established at Highstreet. Results from monitoring activities are reviewed by designated Highstreet personnel, and corrective actions as taken where necessary. **(7.2)**

System Synchronization:

For monitoring processor customer set-up, all clocks on information systems are synchronized via the Network Time Protocol (NTP) to help ensure the integrity and accuracy of processing. **(7.3)**

Monitoring Resource Capacity:

The use of system resources is monitored, tuned and projections are performed by Highstreet Management. Corrective action is taken to ensure that future capacity requirements and system performance objectives are met for key business systems and applications. **(7.4)**

Anti-Virus Protection:

The software Virus Protection Policy requires that Virus screening software be installed and configured to run periodically on all Highstreet mail servers, firewalls, intranet servers, laptops, workstations and desktop machines. Virus detection software must be kept up-to-date using automated means where new virus signatures/virus definitions are added as they are discovered by Virus detection software vendor. **(7.5)**

Backup and Restore:

Highstreet Management has defined backup guidelines for laptops, mobile devices in its Security Policy, and also has defined information backup policies for all critical environments. For critical environments, full tape back-up copies of information and software are taken on a nightly basis using AppAssure, and are tested on a monthly basis by Highstreet (in accordance with the Backup Policy). **(7.6)**

Network Security:

Networks are managed and controlled through the use of firewalls and through defined Access Control Lists (ACL) and Network Address Translation (NAT). Firewalls route external to internal traffic to each VLAN based on ACL rules. Network layer controls limit the ability of an attacker to map the network, find valuable targets and launch attacks without being detected. The firewall also filters packets and protects server sessions. **(7.7)**

Remote Access (VPN and Wireless):

Remote access is controlled through a Virtual Private Network (VPN). Highstreet uses encrypted VPN technology or other similar controls for securing remote network connectivity. All wireless devices utilize the WPA encryption protocol. Additionally, the SSID is not broadcasted. **(7.8)**

Control Objective #8:

- Controls provide reasonable assurance that logical access to the network and other systems and services are restricted to authorized individuals.

Control Activities:

Access Control Policy:

An Access Control Policy is established, documented and reviewed by Highstreet Management, as needed, based on current business and security requirements for access. **(8.1)**

Granting and Revoking User Access:

A formal used registration and de-registration procedure is in place for granting and revoking access to all information systems and services. **(8.2)**

Logoff after User Inactivity:

Unattended computers are set to logoff after 30 minutes of inactivity. **(8.3)**

Access to Network Diagnostic Ports:

Physical and logical access to network diagnostic and configuration ports is restricted from unauthorized access. **(8.4)**

External Network Access:

Groups of information services, users and information systems are segregated from other external network connections, including the Internet. **(8.5)**

Routing Controls:

Routing controls are implemented for networks to ensure that computer connections and information flows do not breach the Access Control Policy of the business applications. **(8.6)**

Authentication (User ID's):

All system users require unique identifier (User ID) to authenticate to systems and applications. **(8.7)**

Password Policy:

Systems for managing passwords are interactive and ensure complex password controls. **(8.8)**

Inactive user sessions will time-out after a defined period of inactivity, and require a password to re-activate the session. **(8.9)**

Control Objective #9:

- Controls within management provide reasonable assurance that security is an integral part of information systems.

Control Activities:

Change Management Policy:

The implementation of changes is controlled through the use of formal change control procedures. **(9.1)**

Control Objective #10:

- Controls within management provide reasonable assurance the information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective actions to be taken.

Control Activities:

Information security events are reported through appropriate Highstreet Management channels for follow-up and resolution in a timely manner. **(10.1)**

Control Objective #11:

- Controls within management provide reasonable assurance that organizational security policies and procedures are in compliance.

Control Activities:

Important records are protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual and business requirements. **(11.1)**

Users are deterred from using information processing facilities for unauthorized purposes. At the system logon prompt, a banner message is displayed to the user that equipment and systems are owned by Highstreet and that unauthorized use is against company policy. **(11.2)**

COMPLEMENTARY USER ENTITY CONTROLS

Highstreet's control structure is designed in such a way as to enable user entities to implement controls in conformity with their internal policies, procedures, and internal control requirements. The application of specified controls at user entities is necessary to achieve the control objectives included in this report.

This section describes controls that may be needed at user entities to complement the controls at Highstreet. The complimentary user entity controls presented below should not be regarded as a comprehensive list of all of the controls that should be employed by user entities. User entity auditors should consider whether the following controls have been placed in operation at user entities. Although Highstreet has designed control procedures which are intended to provide effective control over the processing of user entity transactions, Highstreet cannot be expected to develop control procedures to address all contingencies nor are they able to prescribe or perform the required user procedures, which must take place at the user entities. With these limitations in mind, the following user entity controls have been presented to facilitate user entities to address control issues that are an integral part of the entire control environment in which their data is processed.

The user entity is responsible for the development, implementation, documentation, review, and modification of appropriate internal control procedures to confirm that items and data processed through Highstreet are performed completely, accurately, and in a timely manner. These controls are intended to cover any and all Client provided equipment. Controls which user entities are responsible for include, but are not limited to, the following:

1. User organizations are responsible for understanding and complying with their contractual obligations to Highstreet.
2. User organizations are responsible for determining whether Highstreet security infrastructure is appropriate for its needs and for notifying Highstreet of requested modifications.
3. User organizations are responsible for adhering to Highstreet security procedures, and informing affected vendors of their related responsibilities.
4. Where Clients provide their own or leased equipment, user organizations are responsible for the ensuring their own equipment and resident data is secured, including physical precautions such as locked cabinets. (Highstreet assumes security for only Company-owned systems, information, and equipment.)
5. User organizations are responsible to have appropriate insurance for their own equipment, software and data.
6. User organizations are responsible for informing Highstreet of any regulatory issues which may affect the services provided by Highstreet. (As stated in contract or presented via formal Change Notification. Highstreet will make all attempts to comply within reason.)
7. User organizations are responsible to promptly notify Highstreet of change made to technical or administrative contact information.
8. User organizations are responsible for maintaining and providing Highstreet a list of authorized personnel, vendors and contractors.
9. User organizations are responsible to promptly notify Highstreet to remove terminated employees who are authorized to direct service changes and to modify access authorities.

COMPLEMENTARY USER ENTITY CONTROLS (Continued)

10. User organizations are responsible for ensuring that only authorized individuals have knowledge of their designated personal identification number (PIN), authentication questions, and all other information with an assigned account. (Nimsoft reporting access, setup, and security must be well-documented to support this control. Site support resources are required to comply with Client Security Standards and Practices.)
11. User organizations are responsible for changing their PIN authorization code on a routine basis and notifying Highstreet if the PIN has been compromised. (Nimsoft reporting access, setup, and security must be well-documented to support this control. Site support resources are required to comply with Client Security Standards and Practices.) User organizations are responsible for maintaining their own system(s) of record. *(Dependent on Contract language. If Highstreet has been authorized to maintain a Client System, it must be outlined in the Contract.)*
12. User organizations are responsible for developing their own disaster recovery and business continuity plans that address their inability to access or utilize Highstreet.
13. User organizations are responsible for ensuring the security and integrity of any data or information transmitted via their service or over the Internet, including any data information transmitted. (Highstreet does not access Client Data. Client Security Protocols must be applied by the Client to ensure secure data transmittal.)
14. User organizations are responsible for ensuring that adequate mechanisms are in place to monitor and protect content of any information passing through their network. (Highstreet also uses its own series of Firewalls to provide additional protection.)
15. User organizations are responsible for developing policies and procedures to protect their systems from unauthorized or unintentional use, modification, addition or deletion.
16. User organizations are responsible for creating and communicating specific escalation procedures for problems to their network services and hosts and notifying Highstreet of changes to escalation procedures in a timely manner. (Frequency and method of communication is specified as per contractual language.)
17. User organizations are responsible for implementing their own access control systems on their infrastructure. Highstreet does not maintain or have logical assess to user organization software or data. (Unless specifically provided by Client to Highstreet Site Service Personnel strictly for the purpose of providing repair or upgrade. And only if Client Personnel cannot perform the repair or upgrade actions under Highstreet Personnel direction.)
18. User organizations are responsible for implementing password security practices to their infrastructure and ensuring the confidentiality of any user IDs and passwords assigned to them for use with Highstreet systems. (However, Highstreet also institutes its own password security monitoring and practices as a second level of security (e.g., account lockout).)
19. User organizations are contractually responsible for notifying Highstreet of any specific security requirements to their infrastructure in a timely manner.
20. User organizations are responsible for ensuring the Firewall and system logging are enabled and sufficient for their purposes, where not contracted with Highstreet.
21. User organizations are responsible for ensuring that the impact of scheduled maintenance activities to their production processes and jobs is sufficiently mitigated.
22. User organizations are responsible for notifying or denying requested infrastructure configuration changes in a timely manner.

COMPLEMENTARY USER ENTITY CONTROLS (Continued)

23. If testing is required by contract, user organizations are responsible for notifying and informing Highstreet of the approval or denial of a product solution once testing is completed.
24. User organizations are responsible for notifying Highstreet or required changes to their solutions in a timely manner and for responding to Highstreet inquiries or notifications regarding their solution in a timely manner.
25. User organizations are responsible for notifying Highstreet of suspected or actual network or service problems in a timely manner.
26. User organizations are responsible for monitoring adherence to service level agreements maintained with Highstreet.
27. Outside of contracted monitoring services, user organizations are responsible for implementing monitoring controls to detect and alert the user organization of actual or attempted security breaches to their service (s) or supporting infrastructure. If a Client Site is breached, a mutual responsibility exists to communicate known breaches.
28. User organizations are responsible for timely notification of known or suspected incidents affecting services provided by Highstreet, such as power failure at Client site. User organizations are responsible for timely response to known or suspected incidents reported by Highstreet personnel, such as malicious attacks on Client systems.
29. Encryption controls should in place to protect user organizations and end user sensitive data in storage and transit.

SECTION III - Description of Control Objectives, Tests of Operating Effectiveness and Results of Tests

OBJECTIVE OF OUR EXAMINATION

This report on controls placed in operation and tests of operating effectiveness is intended to provide user entities and their auditors with information sufficient to obtain an understanding of those aspects of Highstreet Services that may be relevant to a user entity's controls for use in a financial statement audit, and potentially reduce the assessed level of control risk below the maximum for certain financial statement assertions.

SCOPE OF THIS REPORT

Our examination was limited to selected Services at the Highstreet Islandia, New York Co-location Facility identified and provided to users and accordingly did not extend to procedures in effect at user entities or other services provided by Highstreet. The examination was conducted in accordance with the Statements on Standards for Attestation Engagements No. 101 ("AT 101") and Service Organization Control ("SOC" 2) established by the American Institute of Certified Public Accountants ("AICPA"). It is each user entity's responsibility to evaluate this information in relation to internal control in place at their user entity to obtain an understanding of controls and assess control risks. The user entities' and Highstreet's portions of the controls must be evaluated together with the user entity's portion of controls. If effective user entity controls are not in place, Highstreet's controls may not compensate for such weaknesses.

Trust Services Principals Tested (in Section III) of this Report

This Report covered 4 for of the 5 Trust Service Principles for SOC 2:

Trust Service Principal	Related Control Reference
Security	Control Objectives: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11
Availability	Control Objectives: 6, 7
Processing Integrity	Control Objective: 7
Confidentiality	Control Objectives: 1, 2, 3, 4, 5, 6, 7, 8, 10, 11

TESTING OF OPERATING EFFECTIVENESS

Our examination included inquiry of management, supervisory, and staff personnel; inspection of documents and records; observation of activities and operations; and re-performance of controls surrounding and provided by Highstreet Services. Our tests of controls were performed on controls as they existed during the period of January 1, 2014 to December 31, 2014, and were applied to those controls relating to control objectives specified by Highstreet. Our examination did not extend to any other activities or service providers.

Results of Testing Performed by eDelta CPA Services, P.C.

Sect	Control Activity	Test of Control Effectiveness	Results
1	**Control Objective:** Controls over the administration, management and support of information security provide reasonable assurance that they are in accordance with business requirements and relevant laws and regulations.		
1.1	A Code of Ethics Policy in the Employee Handbook exists at Highstreet to educate employees on Highstreet's position regarding business ethics, conflicts of interest, compliance with laws, and the handling of confidential and proprietary information. Human Resources is responsible for implementing the Code of Ethics at Highstreet.	Determined through inspection of the Employee Handbook, that it contained Code of Ethics provisions to educate employees on Highstreet's position regarding business ethics, conflicts of interest, compliance with laws, and the handling of confidential and proprietary information. Determined through inquiry of Highstreet Management, that Human Resources was responsible for implementing the Code of Ethics at Highstreet.	No exceptions noted.
1.2	The Security Policy document is approved by Highstreet management, and is published and communicated to all employees and relevant external parties.	Determined through inspection of the Security Policy, that it describes the required attributes, and includes a statement by Highstreet Management indicating its' support for organizational security. Determined through inspection of Security Policy document signatures, that Information Security Awareness education and training programs were provided to Highstreet employees, contractors and relevant third party resources.	No exceptions noted.

Results of Testing Performed by eDelta CPA Services, P.C.

Sect	Control Activity	Test of Control Effectiveness	Results
1	**Control Objective:** Controls over the administration, management and support of information security provide reasonable assurance that they are in accordance with business requirements and relevant laws and regulations.		
1.3	Senior Management meets on a regular basis to discuss and review organizational initiatives that are either planned or in process, as well as to discuss outstanding issues and/or concerns.	Determined though a selected sample of meeting minutes, that IT governance issues/concerns were discussed during Highstreet Executive Committee meetings.	No exceptions noted.
1.4	Service Level Agreements (SLA's) are in effect with Clients and third parties indicating the levels of support to contractors and relevant third parties.	Determined through inspection of a selected sample of SLA Agreements, that required attributes and a statement by Highstreet Management indicating the levels of support to contractors and relevant third parties were in effect.	No exceptions noted.
1.5	Liability Insurance is in effect with declarations supporting reasonable coverage for Highstreet.	Determined through inquiry of Highstreet Management and inspection of the Liability Insurance Policy, that the Policy was in effect during the period under review and contained declarations supporting reasonable coverage.	No exceptions noted.

Results of Testing Performed by eDelta CPA Services, P.C.

Sect	Control Activity	Test of Control Effectiveness	Results
2	**Control Objective:** Controls provide reasonable assurance that a management framework is established to initiate and control the implementation of information security within Highstreet.		
2.1	An information Security Incident Response Policy document is approved by management, published and communicated to all employees and relevant external parties.	Determined through inquiry of Highstreet Management, that the Incident Response Policy was communicated to all employees and third parties. Determined through inspection of the Incident Response Policy that it was approved by Highstreet Management and contained guidelines to identify and act upon significant threats and vulnerabilities.	No exceptions noted.
2.2	The Security Policy clearly defines specific the requirements and responsibilities of information for Highstreet personnel. Formal job descriptions are in place, which define all security roles and responsibilities.	Determined through inquiry of Highstreet Management and inspection of the Security Policy, that the Policy defined specific responsibilities and requirements for Highstreet Information Security personnel. Determined through inquiry of Highstreet Management and inspection of job descriptions that all security roles and responsibilities were defined.	No exceptions noted.

Results of Testing Performed by eDelta CPA Services, P.C.

Sect	Control Activity	Test of Control Effectiveness	Results
2	**Control Objective:** Controls provide reasonable assurance that a management framework is established to initiate and control the implementation of information security within Highstreet.		
2.3	Highstreet's approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes and procedures for information security) are reviewed independently at planned intervals by Management, or when significant changes to the security implementation occur. Alert Logic performs internal scanning.	Determined through inquiry of Highstreet Management and inspection of external and internal (Alert Logic) network security vulnerability reports, that the external network is scanned quarterly and the internal network is scanned annually.	**Exception Noted**: The vulnerability scan reports for the internal and external network, revealed potential issues that may require further investigation and/or remediation actions by Management. **Management Response**: On a go forward basis, per the results of the vulnerability assessment, Management has been applying critical and urgent patches on an ongoing basis. Vulnerability scanning occurs every 15 days, at which point the updated reports are evaluated and additional remediation action is taken. As a long-term solution, Management will implement an automated solution utilizing a third party patch management tool. This will be used for the automated scheduling and installation of critical patches.

Results of Testing Performed by eDelta CPA Services, P.C.

Sect	Control Activity	Test of Control Effectiveness	Results
3	**Control Objective:** Controls over organizational assets provide reasonable assurance that they are properly classified to protect against their misuse.		
3.1	Rules for the acceptable use of information and assets associated with information processing facilities are identified, documented in the Acceptable Use Policy, and are implemented by Highstreet Management.	Determined through inspection of a selected sample of employee signed Security Policy acceptances, that Highstreet Management has documented, developed, and published a formal Acceptable Use Policy Determined through inquiry of Highstreet Management, that the Security Policy communicated to employees.	No exceptions noted.
3.2	Information Systems Management and Administration Information is classified in terms of its value, legal requirements, sensitivity and criticality to Highstreet.	Determined through inspection of the published Information Classification Policy and the Security Policy, that information was classified in terms of its value, legal requirements, sensitivity and criticality to Highstreet.	No exceptions noted.

Results of Testing Performed by eDelta CPA Services, P.C.

Sect	Control Activity	Test of Control Effectiveness	Results
4	**Control Objective:** Controls over disciplinary actions and the termination of employees, contractors, and 3rd party users provide reasonable assurance to reduce the risk of theft, fraud or misuse of facilities.		
4.1	Members of Senior Management are engaged when recurring performance concerns are identified. Annual performance reviews are completed for selected Departments within Highstreet, such as, NOC, Back Office Processing, and Field Services. Responsibilities for performing employment termination or change of employment are clearly defined, assigned and documented by Management.	Determined through inspection of a selected sample of termination check lists and annual performance reviews for employees, contractors, consultants and other third party resources, that Highstreet Management followed the appropriate guidelines for the termination process.	No exceptions noted.
4.2	There is a formal disciplinary process for employees who have committed a security breach. This disciplinary action is documented in the Security Policy.	Determined through inspection of a sample selection of termination check lists, that there was a formal disciplinary process for employees who have committed a security breach. Determined through inspection of the Security Policy, that disciplinary action was documented.	No exceptions noted.

Results of Testing Performed by eDelta CPA Services, P.C.

Sect	Control Activity	Test of Control Effectiveness	Results
5	**Control Objective:** Controls provide reasonable assurance that physical access to organizational premises, data center facilities and other sensitive operational areas are restricted to authorized users.		
5.1	Security perimeters, including barriers such as walls and manned reception desks are used to protect areas that contain Highstreet information and the information processing facilities.	Determined through observation the existence of security perimeters, including barriers such as walls and manned reception desks to protect areas that contain Highstreet information and information processing facilities.	No exceptions noted.
5.2	Physical access to the Highstreet building facility is restricted through card key access. Access to the NOC is restricted through both card key and biometric access.	Determined through inquiry and observation, that physical access to the building facility was restricted by card key access, and that the NOC was restricted through card key and biometric access. Determined through inspection of the card key access rules, that access to sensitive areas are restricted to authorized individuals only.	No exceptions noted.
5.3	Visitors and vendors entering the Highstreet building facility must go to the reception desk where they enter their name, company information, the reason for their visit, and the time of their visit and date in a sign-in log.	Determined through observation of the reception desk and inspection of a selected sample of reception desk sign-in logs, that visitors and vendors entering the building facility reported to the reception desk, where they enter their name, company information, reason for their visit, the time of their visit and date in the sign-in log.	No exceptions noted.
5.4	The receptionist contacts the appropriate Highstreet representative who escorts the vendor or visitor to the appropriate location.	Determined through observation and inspection of a selected sample of receptionist visitor logs, that the receptionist contacted the appropriate Highstreet representative who escorted the visitor to the appropriate location.	No exceptions noted.

Results of Testing Performed by eDelta CPA Services, P.C.

Sect	Control Activity	Test of Control Effectiveness	Results
5	**Control Objective:** Controls provide reasonable assurance that physical access to organizational premises, data center facilities and other sensitive operational areas are restricted to authorized users.		
5.5	Visitors and vendors are required to wear an ID badge which identifies them to Highstreet personnel.	Determined through observation and inspection of access logs and procedures, that access to organizational premises, data center facilities and other sensitive operational areas were restricted. Determined through observation, that visitors and vendors were required to wear an ID badge and sign-in to identify themselves to Highstreet personnel.	No exceptions noted.
5.6	Physical access to the Highstreet building facility and the NOC are monitored and reviewed on a periodic basis by Highstreet Management for any unusual activity.	Determined through inspection of a sample of card key access logs, that physical access to the Highstreet building facility and NOC was monitored and reviewed by Highstreet Management for any unusual activity.	No exceptions noted.
5.7	Video surveillance cameras are in place to monitor any unusual activity for the Highstreet building facility and NOC.	Determined through observation and inspection of a sample of video surveillance monitoring logs, that video surveillance cameras were in place to monitor any unusual activity for the Highstreet building facility and NOC. Determined through inquiry of Highstreet Management that security surveillance equipment was inspected and maintained to ensure proper operation.	No exceptions noted.

Results of Testing Performed by eDelta CPA Services, P.C.

Sect	Control Activity	Test of Control Effectiveness	Results
5	**Control Objective:** Controls provide reasonable assurance that physical access to organizational premises, data center facilities and other sensitive operational areas are restricted to authorized users.		
5.8	The Highstreet building facility and the NOC are alarmed for physical security breaches. Should an intruder break-in take place, a message is sent to the proper authorities (i.e., the police and fire departments) for further action.	Determined through observation and inspection of physical access logs, that the Highstreet building facility and NOC were alarmed and configured to send a message to the proper authorities should an intruder break-in occur. Determined through inquiry of Highstreet Management, that security detection equipment was inspected and maintained to ensure proper operation.	No exceptions noted.
5.9	Access points, such as delivery and loading areas and other points (where unauthorized persons may enter the premises) are segregated from the Highstreet information processing facilities to help avoid unauthorized access.	Determined through observation, that delivery and loading areas and other access points, were segregated from Highstreet information processing facilities to reduce the risk of unauthorized access.	No exceptions noted.
5.10	Equipment, information and software are not taken off-site without prior authorization from Highstreet Management.	Determined through inspection of asset removal logs and related documentation, that equipment, information and software were not taken off-site without prior authorization from Highstreet Management. Determined that Highstreet Management performed an Asset Audit to verify that the proper equipment was taken offsite. Obtained and reviewed samples of equipment decommissioned on the security infrastructure side of the business during the review cycle.	No exceptions noted.

Results of Testing Performed by eDelta CPA Services, P.C.

Sect	Control Activity	Test of Control Effectiveness	Results
6	**Control Objective:** Controls provide reasonable assurance that environmental controls are established within the data center and processing facilities to protect physical assets.		
6.1	The Highstreet Data Center is cooled by a separate refrigeration system that is connected to separate backup natural gas generators should an electrical outage occur.	Determined through observation and inspection of the Highstreet cooling diagram, that the Highstreet Data Center was cooled by a separate refrigeration system, which was connected to separate backup natural gas generators. Determined through inquiry of Highstreet Management and review of maintenance records, that backup generators were tested on a quarterly basis.	No exceptions noted.
6.2	The Data Center and administrative offices are protected by a Novec fluid system which extinguishes by removing heat from the fire. The Data Center also has a fire alarm that is monitored by a central station on a 24 by 7 basis.	Determined through observation and inspection of the fire alarm diagram, that the Data Center and administrative offices were protected by a Novec fluid system. Determined through observation and inspection of central station monitoring documentation, that the Data Center had a fire alarm system that was monitored by a central station on a 24 by 7 basis.	No exceptions noted.
6.3	Water detection sensors are provided in the Data Center and alerts are sent to Highstreet Management should water be detected.	Determined through inquiry and inspection, that water detection sensors were provided in the Data Center and it was configured to send alerts to Highstreet Management for any unusual conditions.	No exceptions noted.

Results of Testing Performed by eDelta CPA Services, P.C.

Sect	Control Activity	Test of Control Effectiveness	Results
6	**Control Objective:** Controls provide reasonable assurance that environmental controls are established within the data center and processing facilities to protect physical assets.		
6.4	Heat detection sensors are provided in the Data Center and alerts are sent to Highstreet Management for any unusual at temperature conditions.	Determined through inquiry and observation, that heat detection sensors were provided in the Data Center. Determined through inspection of heat system sensors, that they were configured to send alerts to Highstreet Management for unusual temperature conditions.	No exceptions noted.
6.5	Equipment is protected from power failures and other disruptions caused by failures in supporting utilities, through an Uninterrupted Power Supply (UPS), which is phased to a backup gas generator to help ensure continued operations.	Determined through inquiry and observation, that a UPS system and a backup gas generator was in place and operational to help support the continued operation of critical systems. Verified that the gas generator was tested on a weekly basis to startup within 15 seconds after the UPS system is enabled.	No exceptions noted.
6.6	Emergency lighting exists in the Data Center as well as core information processing facilities in the event of a major power failure.	Determined through inquiry and observation, that emergency lighting existed in the Data Center as well as core information processing facilities in the event of major power failures.	No exceptions noted.
6.7	Power and telecommunications lines into Highstreet Data Center and core information processing facilities are buried underground to reduce the risk of significant damage to them.	Determined through inquiry and observation, that power and telecommunications lines into Data center and core information processing facilities were underground, and that redundant power feeds existed into two separate power utilities.	No exceptions noted.

Results of Testing Performed by eDelta CPA Services, P.C.

Sect	Control Activity	Test of Control Effectiveness	Results
6	**Control Objective:** Controls provide reasonable assurance that environmental controls are established within the data center and processing facilities to protect physical assets.		
6.8	Paper documents and other flammable materials are kept outside of the Highstreet Data Center and core information processing facilities. Aisles and major walkways are also free from obstruction and other electrical hazards.	Determined through inquiry and observation, that paper documents and other flammable materials were kept outside of the Data Center and core information processing facilities. Observed that aisles and major walkways were free from obstruction and other electrical hazards.	No exceptions noted.

Results of Testing Performed by eDelta CPA Services, P.C.

Sect	Control Activity	Test of Control Effectiveness	Results
7	**Control Objective:** Controls over the operation and monitoring of information systems provide reasonable assurance that data is processed completely and securely.		
7.1	Changes to information processing facilities and systems are documented, and require formal authorization and approval from Highstreet Management on the change control tracking form before they are implemented.	Determined through inquiry of Highstreet Management, inspection of Highstreet Policy and a selected sample selection of meeting minutes, that changes to information processing facilities and systems are documented and required formal authorization and approval from Highstreet Management.	No exceptions noted.
7.2	Procedures and automated tools for monitoring the use of information processing facilities are established at Highstreet. Results from monitoring activities are reviewed by designated Highstreet personnel, and corrective actions as taken where necessary.	Determined through inspection of a selected sample of monthly monitoring reports and system monitoring tools, that Highstreet Management and designated staff regularly reviewed system use information and performed corrective actions as necessary.	No exceptions noted.
7.3	For monitoring processor customer set-up, all clocks on information systems are synchronized via the Network Time Protocol (NTP) to help ensure the integrity and accuracy of processing.	Determined through inspection of NTP settings and formal procedures, that time drift was checked to ensure that servers are synchronized to the NTP for customer set-up.	No exceptions noted.
7.4	The use of system resources is monitored, tuned and projections are performed by Highstreet Management. Corrective action is taken to ensure that future capacity requirements and system performance objectives are met for key business systems and applications.	Determined through inspection of a sample of monthly system monitoring reports and meeting records, that Highstreet Management monitored and provided reasonable actions to ensure the availability and efficiency of key systems/applications.	No exceptions noted.

Results of Testing Performed by eDelta CPA Services, P.C.

Sect	Control Activity	Test of Control Effectiveness	Results
7	**Control Objective:** Controls over the operation and monitoring of information systems provide reasonable assurance that data is processed completely and securely.		
7.5	The software Virus Protection Policy requires that Virus screening software be installed and configured to run periodically on all Highstreet mail servers, firewalls, intranet servers, laptops, workstations and desktop machines. Virus detection software must be kept up-to-date using automated means where new virus signatures/virus definitions are added as they are discovered by Virus detection software vendor.	Determined through inspection of the Virus Protection Policy and a sample of monthly monitoring reports and Virus software settings, that Virus protection software was kept up-to-date to detect malicious code. Determined through inspection of a sample of Virus software logs, that electronic mail attachments were checked for malicious and mobile code risks.	No exceptions noted.
7.6	Highstreet Management has defined backup guidelines for laptops, mobile devices in its Security Policy, and also has defined information backup policies for all critical environments. For critical environments, full tape back-up copies of information and software are taken on a nightly basis using AppAssure, and are tested on a monthly basis by Highstreet (in accordance with the Backup Policy).	Determined through inspection of Highstreet guidelines and a sample of backup logs, that Highstreet performs full nightly backups, and tests backup media and information on a monthly basis to ensure that data was backed-up in a complete and accurate manner.	No exceptions noted.

Results of Testing Performed by eDelta CPA Services, P.C.

Sect	Control Activity	Test of Control Effectiveness	Results
7	**Control Objective:** Controls over the operation and monitoring of information systems provide reasonable assurance that data is processed completely and securely.		
7.7	Networks are managed and controlled through the use of firewalls and through defined Access Control Lists (ACL) and Network Address Translation (NAT). Firewalls route external to internal traffic to each VLAN based on ACL rules. Network layer controls limit the ability of an attacker to map the network, find valuable targets and launch attacks without being detected. The firewall also filters packets and protects server sessions.	Determined through inspection of the approved network and firewall security matrix and network diagrams, that network controls, including: ACL's, NAT, VLAN's, network layer control limits and filters were in place to provide security, integrity and availability of information transmitted over the network.	No exceptions noted.
7.8	Remote access is controlled through a Virtual Private Network (VPN). Highstreet uses encrypted VPN technology or other similar controls for securing remote network connectivity. All wireless devices utilize the WPA encryption protocol. Additionally, the SSID is not broadcasted.	Determined through inquiry, observation and inspection of security configurations and network diagrams, that Highstreet used encrypted VPN technology or other similar controls for securing remote network connectivity. Determined through inquiry and observation of wireless configurations, that all wireless devices utilized encryption with TKIP plus MAC Addressing Filtering, required separate authentication, and that the SSID was not broadcasted.	No exceptions noted.

Results of Testing Performed by eDelta CPA Services, P.C.

Sect	Control Activity	Test of Control Effectiveness	Results
8	**Control Objective:** Controls provide reasonable assurance that logical access to the network and other systems and services are restricted to authorized individuals.		
8.1	An Access Control Policy is established, documented and reviewed by Highstreet Management, as needed, based on current business and security requirements for access.	Determined through inspection of the Access Control Policy, that it established security requirements for access based on business requirements. Compared an authorized listing of access rights to assigned rights, and verified that the job descriptions and assigned roles matched.	No exceptions noted.
8.2	A formal used registration and de-registration procedure is in place for granting and revoking access to all information systems and services.	Determined through inspection of a sample of new hires and termination documentation, that access was properly revoked or granted based on the formal approval.	No exceptions noted.
8.3	Unattended computers are set to logoff after 30 minutes of inactivity.	Determined through observation of unattended computers, and inspection of the online Windows Group Policy settings, that computers were set to logoff after 30 minutes of inactivity.	No exceptions noted.
8.4	Physical and logical access to network diagnostic and configuration ports is restricted from unauthorized access.	Determined through inspection of firewall login name and password access settings and observation of physical access to network devices, that physical and logical access was restricted to specific configuration ports.	No exceptions noted.

Results of Testing Performed by eDelta CPA Services, P.C.

Sect	Control Activity	Test of Control Effectiveness	Results
8	**Control Objective:** Controls provide reasonable assurance that logical access to the network and other systems and services are restricted to authorized individuals.		
8.5	Groups of information services, users and information systems are segregated from other external network connections, including the Internet.	Determined through inspection of the network diagram and access control lists, that the Highstreet internal network was separate from other external network connections and the Internet.	No exceptions noted.
8.6	Routing controls are implemented for networks to ensure that computer connections and information flows do not breach the Access Control Policy of the business applications.	Determined through inspection of network access control lists, that they were configured to allow authorized destination addresses only and exclude all others.	**Exception Noted**: We noted one network device accessing the ID: "CNS" that was being shared by three individuals in order to to gain privileged access to the core Firewall. **Management Response**: Management plans on establishing individual access accounts to the core firewall and router.
8.7	All system users require unique identifier (User ID) to authenticate to systems and applications.	Determined through inspection of user access lists, that all users have a unique identifier (user ID) for their personal use, and that a suitable authentication technique was chosen to substantiate the claimed identity of a user.	No exceptions noted.

Results of Testing Performed by eDelta CPA Services, P.C.

Sect	Control Activity	Test of Control Effectiveness	Results
8	**Control Objective:** Controls provide reasonable assurance that logical access to the network and other systems and services are restricted to authorized individuals.		
8.8	Systems for managing passwords are interactive and ensure complex password controls.	Determined through inspection of the password management system and Windows passwords require complex passwords.	No exceptions noted.
8.9	Inactive user sessions will time-out after a defined period of inactivity, and require a password to re-activate the session.	Determined through inspection of the Windows password policy, that inactive user sessions timed-out after a defined period of inactivity and required a password to re-activate the session.	No exceptions noted.

Results of Testing Performed by eDelta CPA Services, P.C.

Sect	Control Activity	Test of Control Effectiveness	Results
9	**Control Objective:** Controls within management provide reasonable assurance that security is an integral part of information systems.		
9.1	The implementation of changes is controlled through the use of formal change control procedures.	Determined through inspection of Highstreet Policy, a selected sample of changes, change assessment worksheets, and meeting minutes, that formal change control procedures were followed.	No exceptions noted.

Results of Testing Performed by eDelta CPA Services, P.C.

Sect	Control Activity	Test of Control Effectiveness	Results
10	**Control Objective:** Controls within management provide reasonable assurance the information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective actions to be taken.		
10.1	Information security events are reported through appropriate Highstreet Management channels for follow-up and resolution in a timely manner.	Determined through inspection of the Incident Response Policy, and a selected sample of security committee meeting minutes, that the incident reporting process was documented and contained escalation plans and procedures to address events in a timely manner. There were no incidents recorded during the period under review.	No exceptions noted.

Results of Testing Performed by eDelta CPA Services, P.C.

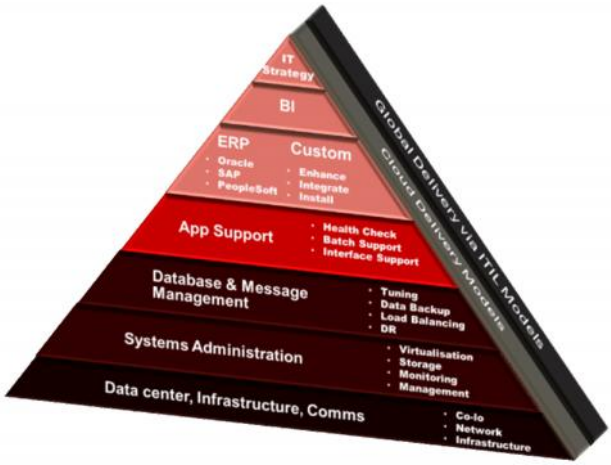
Sect	Control Activity	Test of Control Effectiveness	Results
11	**Control Objective:** Controls within management provide reasonable assurance that organizational security policies and procedures are in compliance.		
11.1	Important records are protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual and business requirements.	Determined through inspection of the Highstreet Retention Policy, record retention table, shredding policy, certifications of shredded documents and locked shredding bins, that confidential information was protected.	No exceptions noted.
11.2	Users are deterred from using information processing facilities for unauthorized purposes. At the system logon prompt, a banner message is displayed to the user that equipment and systems are owned by Highstreet and that unauthorized use is against company policy.	Determined through inspection of the Highstreet Domain Policy, that it was communicated to users and provided guidelines for the proper use of facilities. Observed a user login to information systems, and noted that it displayed a warning banner message: that the equipment and systems are owned by Highstreet and that unauthorized use is against company policy.	No exceptions noted.

SECTION IV - Additional Information Provided by Highstreet (Subsequent Events)

Effective March 1, 2014, Highstreet joined the Cloud Division of Highstreet IT Solutions, LLC. Highstreet is a Denver-based IT service provider which specializes in full life-cycle application management for Oracle PeopleSoft, Oracle EBS, and SAP applications. This information is presented by Highstreet to provide additional information to user organizations, and is not a part of Highstreet's description of controls placed in operation.

Through its acquired operations, Highstreet has been providing application management, remote infrastructure management (RIM), equipment maintenance, product procurement, and hosting services supported by a 24x7x365 service desk since 1999.

Highstreet's ERP hosting solutions include all required technical services to host and support an ERP environment: data center, infrastructure, network, OS/virtualization, database, and application operation services. Highstreet maintains and operates a dedicated private cloud, custom-built to deliver ERP solutions. By leveraging the latest in cloud technologies, we are able to offer market leading SLAs on end-to-end application availability as well as transaction performance.



Highstreet's Cloud Services Division provides a full complement of application hosting and IT operations services on a flexible engagement model. Our specialty is helping our customers realize value from cloud technologies – whether delivered in a private cloud (your data center or ours), public cloud, or a hybrid cloud. Our services can be engaged a la carte in either a consultative, project, or operative agreement. Our capabilities start with robust monitoring tools which monitor physical IT assets and application performance.

We offer a full range of hosting (IaaS and PaaS; physical and virtual), database administration, and application operations services, delivered in-line with the ITIL framework. Our confidence in our operative services allows us to deliver business application SLAs which are aligned to the outcomes IT must deliver to the business.